IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

CRYSTAL BYRD, et al.,	)	
	)	
Plaintiffs,	)	**Civil Action No. 11-101 Erie**
	)	
vs.	)	**District Judge Bissoon**
	)	
AARON'S, INC., et al.,	)	**Magistrate Judge Baxter**
	)	
Defendants.	)	

MAGISTRATE JUDGE'S REPORT AND RECOMMENDATION
On Plaintiff's Renewed Motion to Certify Class

I. RECOMMENDATION

In this putative class action lawsuit, Plaintiffs Crystal Byrd and her husband, Brian Byrd, claim that Defendants Aaron's, Inc. and its franchisee, Aspen Way Enterprises, Inc., violated the Electronic Communications Privacy Act, 18 U.S.C. §2510 *et seq.*, through the use of alleged spyware known as "PC Rental Agent." Presently pending before the Court is the Plaintiffs' renewed motion to certify the class [ECF No. 439]. For the reasons that follow, it is respectfully recommended that the Plaintiffs' motion be denied.

II. REPORT

A. Relevant Procedural and Factual Background

1. The Background Facts

Aaron's Inc. ("Aaron's") operates company-owned stores and also oversees independently-owned franchise stores that sell and lease home computers, among other items. ECF No. 296, Corrected Third Amended Complaint, ¶11. Aspen Way Enterprises, Inc. ("Aspen Way") is a Montana franchisee of Aaron's doing business in Wyoming and other states. *Id.* ¶15.

In July 2010, Plaintiff Crystal Byrd (hereafter, at times, "Crystal") entered into a lease agreement to rent a laptop computer from Aspen Way. *Id.* ¶ 118. Although Crystal subsequently made payments in full compliance with the rental agreement, *id.* ¶120, an agent of Aspen Way attempted to repossess the laptop from the Byrds' home on or about December 22, 2010. *Id.* ¶124. At that time, the agent presented a screenshot of a poker website that Plaintiff Brian Byrd (hereafter, at times, "Brian") had visited, along with a picture that the laptop's camera had taken of him while playing poker online. *Id*. ¶¶ 122, 124.

Aspen Way had obtained the picture and screenshot through the company's use of certain software designed by DesignerWare, LLC and named "PC Rental Agent" (hereafter, "PCRA"). *Id.* ¶¶ 83-84, 121-122. This software had an optional function called "Detective Mode" which, when downloaded and activated, could collect screenshots, keystrokes, and webcam images from the computer and its users. *Id.* ¶¶ 88-89. Plaintiffs contend that, between November 16, 2010 and December 20, 2010, Detective Mode secretly accessed their laptop on 347 occasions over the course of eleven different days, capturing a variety of private, and sometimes, sensitive information. *Id*. at ¶ 123.

2. <u>The Litigation</u>

In May 2011, Plaintiffs commenced this litigation with the filing of a putative class action suit against Aaron's, Aspen Way, and various other parties. ECF No. 1. Following protracted pretrial proceedings, much of which are presently irrelevant, Plaintiffs filed their "Corrected Third Amended Complaint," ECF No. 296, which remains the operative pleading at

this juncture. Therein, they assert claims against Aaron's and Aspen Way for alleged violations of the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §2510 *et seq*.[1]

Plaintiffs claim that, beginning in 2007, franchise field consultants employed by Aaron's started encouraging Aaron's franchisees to explore the possibility of using PCRA. ECF No. 296, ¶82. Beginning in June of 2009, Aaron's franchisees began secretly installing PCRA on rent-to-own computers. *Id.* ¶ 84. PCRA allows its installer (here, the rent-to-own store) to remotely and surreptitiously build and activate the Detective Mode function on the laptop over the Internet and through the Aaron's Inc. and DesignerWare websites. *Id.* ¶ 88. After Detective Mode is built onto a laptop, the installer is able to activate it and to choose various levels of surveillance. *Id*. at ¶ 89. The installer may secretly have photos taken through the computer's webcam, as well as capture keystrokes and take screen shots. *Id*. at ¶¶ 3, 84, 89.

Plaintiffs allege that Aaron's Inc. has expressly consented to have its franchisee stores access and use the DesignerWare and PC Rental Agent websites through the Aaron's Inc. corporate intranet and server to spy on unsuspecting customers. *Id.* at ¶ 137. This remote access has resulted in "several hundred thousands of occasions" when stores secretly gathered information from the computer user. *Id*. at ¶ 137. Plaintiffs claim that Aspen Way alone collected personal and private information from its customers' laptops on more than 50,000 occasions. *Id*. at ¶ 138. Plaintiffs further claim that approximately 167 Aspen Way computers were subjected to surveillance through use of the Detective Mode function of PCRA. ECF No. 293-11; *see* also ECF No. 440-9.

[1] The CTAC originally named more than fifty other independent franchisees of Aaron's as defendants in this lawsuit. It also included claims for common law invasion of privacy, conspiracy, and aiding and abetting. Following the District Court's ruling on March 31, 2014, however, the only remaining Defendants are Aaron's and Aspen Way, and the only remaining claims are those alleging direct violations of the ECPA. *See* Order dated 3/31/14, ECF No. 339, adopting Report and Recommendation, ECF No. 318.

3. The Original Class Certification Motion

Plaintiffs originally moved for class certification on July 1, 2013. ECF No. 174. In a Report and Recommendation issued on January 31, 2014, the undersigned recommended that the motion be denied on the ground that the proposed class, as then defined by Plaintiffs, was not ascertainable. ECF No. 319. The District Court subsequently adopted this Court's Report and Recommendation on March 31, 2014. ECF No. 340.

On appeal, the U.S. Court of Appeals for the Third Circuit reversed the District Court's order and remanded the case for further proceedings. The Third Circuit addressed the ascertainability requirement as it pertained to the following proposed class:

> Class I—All persons who leased and/or purchased one or more computers from Aaron's, Inc., and their household members, on whose computers DesignerWare's Detective Mode was installed and activated without such person's consent on or after January 1, 2007.
>
> Class II—All persons who leased and/or purchased one or more computers from Aaron's, Inc. or an Aaron's, Inc. franchisee, and their household members, on whose computers DesignerWare's Detective Mode was installed and activated without such person's consent on or after January 1, 2007.

As an initial matter, the Third Circuit rejected the notion that the "underinclusivity" of a proposed class definition is relevant to considerations of ascertainability. 784 F.3d at 167 ("We decline to engraft an "underinclusivity" standard onto the ascertainability requirement."). To the extent the Defendants argued that the proposed classes were overbroad because, *e.g.*, they included putative class members who lacked standing or had not been injured, the Third Circuit admonished that these types of concerns should be addressed in the context of Rule 23(b)(3)'s "predominance" requirement and Article III standing. *Id.* at 168. The Third Circuit then went on to hold that the proposed classes consisting of "owners" and "lessees, as well as their "household members," were ascertainable. *Id.* at 169. The Third Circuit remanded the case so

that the District Court could reevaluate Rule 23's other criteria in the first instance. *Id.* at 171-72.

4. The Renewed Motion for Class Certification

Following remand, this Court held a status conference reopening discovery and setting deadlines for class certification briefing. ECF No. 372. Thereafter, major discovery disputes ensued necessitating the postponement of the class certification briefing schedule multiple times. After numerous hearings and several extensions, finally, after eighteen months, Plaintiffs filed their Renewed Motion for Class Certification and supporting materials on October 14, 2016. ECF Nos. 439-442. In their motion, they define the putative class as:

> All persons who leased and/or purchased one or more computers from Aaron's, Inc. and/or Aspen Way Enterprises, Inc., and their household members, on whose computers Designerware's Detective Mode was installed and activated without such person's consent on or after January 1, 2007.

ECF No. 439. Plaintiffs contend that certification is appropriate under either Federal Rule of Civil Procedure 23(b)(2) or 23(b)(3).[2]

Among the materials that Plaintiffs have submitted in support of their motion is Aspen Way's "Response to Civil Investigative Demand" by the Federal Trade Commission. ECF No. 440-8. In relevant part, the response states:

> The PC Rental Agent software was marketed by Designerware as a means of reducing losses stemming from customers who defaulted on their rental obligations and/or to find and recover lost and stolen computers. The PC Rental Agent software is provided to Aspen Way by Designerware on a single CD Rom. The CD Rom is sent to each Aspen Way store location via U.S. Postal Mail. When Aspen Way's stores receive the PC Rental Agent by U.S. Postal Mail, store employees then utilize the CD Rom to install the software on Aspen Way's computers. Updates are

[2] Despite the extended period of discovery, Plaintiffs' renewed motion is substantially similar to the original motion, especially in relation to the predominance argument.

automatically sent by Designerware to Aspen Way on CD Rom via U.S. Postal Mail.

When a consumer reports to Aspen Way that a computer has been lost or stolen, Aspen Way requests that the customer go to the local law enforcement agency and file a police report, which Aspen Way requests that the customer then bring to the local store. After receiving the police report, the store General Manager provides the information to John Pollock [Aspen Way's former Director of Operations], who determines what features of the PC Rental Agent software to utilize.

The PC Rental Agent software first provides Aspen Way the ability to lock-down an Aspen Way computer if a customer defaults on his or her lease or if an Aspen Way computer is reported as lost or stolen. This feature is most utilized upon default, to compel a customer to call into the store location and make payment. In the case of a lost or stolen computer, PC Rental Agent also provides Aspen Way the ability to locate an Aspen Way computer by automatically tracking the GPS coordinates of the computer, so long as the computer is connected to the internet by the user. The GPS coordinates do not identify a specific address; rather, they merely provide the longitude and latitude of the location of the Aspen Way computer. In order to more specifically identify the location of its computer, Aspen Way has to enter the coordinates into a search engine (e.g. *Google Maps*), which may then assist in locating an approximate address. Aspen Way's general managers can access the PC Rental Agent for these purposes, but they do not have access to Detective Mode.

PC Rental Agent also offers features through the Detective Mode, which are activated online through the PC Rental Agent website. The Detective Mode of PC Rental Agent presently offers four options. Option One transmits 30 screen shots, which are taken when the person using the computer logs onto the computer, at one second intervals for 30 seconds. Depending upon whether the computer is being used through a landline or via wireless connections, the GPS coordinates may identify a specific real property address, or the coordinates may only generally identify an area where the computer is located. Option Two transmits continuous screen shots of the user's activities, which, in the specific case of Aspen Way's usage of PC Rental Agent, are transmitted to the email address of John Pollock. Mr. Pollock then reviews the screen shots to determine if any identifying information is available to assist in locating the computer and/or to provide to law enforcement in helping to track down the lost or stolen computer. Option Three transmits keystrokes of identifying information from the user, including address and phone number. On the user's end, the user is asked to type in identifying information into a license form, which is then transmitted to PC Rental Agent and emailed to Mr. Pollock. In the specific case of Aspen Way's usage of PC Rental

> Agent, this information is then transmitted via email to John Pollock. It is the practice of Aspen Way to provide only relevant information to employees involved in collection which will assist them in their collection duties. It is not the practice of Aspen Way to actually provide these employees with the actual screen shots – only any relevant information obtained from those screen shots. Finally, Option Four of the Detective Mode shuts down the computer and provides a separate option to transmit a web photo, showing who is using the computer at the time of shut-down.
>
> Various factors are considered by Mr. Pollock in determining what level of Detective Mode should be activated. Where Aspen Way has reason to believe that a customer is misleading Aspen Way or law enforcement about a computer being lost or stolen, and where Options One and Two did not yield information that allowed the computer to be recovered, Options Three or Four may be utilized. Factors which Aspen Way considers in deciding what information should be transmitted include, but are not limited to: level of account delinquency, resistance by the customer to submit a police report, information from a law enforcement agency that suggests the customer is not being honest about a computer being lost or stolen, field visits which garner information that the computer is still in the customer's possession, third party information disclosing that the customer may still be in possession of the computer, GPS Coordinates that identify the customer's home as the location for the computer, information gathered in the ordinary course of collection activities that suggests the customer is still in possession of the computer, and information/requests from law enforcement.
>
> PC Rental Agent also has a feature that allows the computer to be "locked-down." This feature automatically activates when the computer has not been logged-onto after a set interval of time (generally, every 45 to 90 days). Aspen Way has the ability to uninstall the software to deactivate this feature, which it will do in cases where a customer might not be utilizing the internet, to avoid the lock-down feature preventing use by the customer of the computer. This feature is helpful in situations where computers are pawned and are not being utilized in the pawn location.

ECF No. 440-8, at 6-7.

Plaintiffs have also proffered the September 19, 2013 "declaration" of Micah Sherr, Ph.D., which is in the nature of an expert report, and which had previously been submitted in

connection with the Plaintiff's original motion for class certification.[3] ECF No. 440-2. In his report, Dr. Sherr explains the method by which PCRA and Detective Mode were used to surreptitiously obtain information from computers that were purchased and leased by Aspen Way customers. Because Plaintiffs rely heavily on Dr. Sherr's report, and because the report is central to questions of commonality and predominance under Rule 23(b)(3), this Court will discuss his analysis at length.[4]

Dr. Sherr begins by discussing the architecture and functionality of Aaron's PCRA/Detective Mode System (the "system") and describes how it was used in concert by Aaron's and its franchisees. ECF No. 440-2 ¶10. As explained by Dr. Sherr, the system is comprised of the PCRA software, the Detective Mode software, the DesignerWare website and database server, and an email server operated by Aaron's Corporate, all of which are integrated and act collectively to perform monitoring and interception functions. *Id.* ¶¶ 9, 16-18.

Dr. Sherr describes the process whereby Aaron's or its franchisees would activate Detective Mode on the computers of its customers. First, the relevant rent-to-own store (here, Aspen Way) would purchase the PCRA software from DesignerWare and install it on the computer prior to rental by the customer. *Id.* ¶20. Once installed, PCRA would run whenever the computer was powered on. It would periodically signal a database server operated and

[3] The Court notes that, in connection with the present class certification proceedings, Dr. Sherr submitted a second report (the "New Sherr Report"), dated December 1, 2016. ECF No. 463-5. By Memorandum Opinion and Order entered on March 22, 2107 and subsequently affirmed by the District Court, ECF Nos. 496, 497, and 506, the undersigned granted Defendants' motion to strike the New Sherr Report. Accordingly, this Court has not considered or relied on any aspect of the New Sherr Report in this Report and Recommendation.

[4] Dr. Sherr's declaration is currently filed under seal, as it includes exhibits of a sensitive nature. The declaration was originally filed on September 23, 2013 in redacted form, ECF No. 293-2, and that version remains unsealed. Here, the Court cites only the information from Dr. Sherr's declaration that is already publicly available at ECF No. 293-2.

maintained by DesignerWare whenever certain events (such as joining a new network) occurred, assuming the computer was connected to the internet. *Id*. ¶ 21. To activate Detective Mode, the store employee would access DesignerWare's web portal. From there, the employee could remotely enable Detective Mode on a chosen computer and specify the various functions of Detective Mode that should be activated on that particular computer. *Id*. ¶¶23-24. PCRA would then be instructed, the next time it connects to the DesignerWare database, to surreptitiously install and activate Detective Mode on the computer with the specific functions selected by the employee. *Id*.

Once installed and activated, Detective Mode captures the computer operator's keystrokes as they occur. *Id*. ¶27, 29. It also captures "screenshots" – i.e. the contents of the computer's display – every two minutes. *Id*. ¶30. In addition, depending on the mode of the program that is being used, Detective Mode may capture the contents of a computer's text-based clipboard. *Id*. ¶29, n.9. Under one particular operating mode, Detective Mode can surreptitiously take photos of the user or the surrounding area if a functional camera is present on the computer. *Id*. ¶31. Finally, the system can attempt to discover the physical location of the computer by using wireless networks to track the computer's latitude and longitude. *Id*. ¶32.

Within a given two-minute interval in which it is active, Detective Mode records all keystrokes, captures a screenshot of the computer's display, and (optionally) takes a photo using the webcam and/or records the contents of the clipboard. *Id*. ¶35.) When the computer is connected to the internet, Detective Mode surreptitiously forwards this information to the DesignerWare server every two minutes. *Id*. ¶38. From there, the information is forwarded to the store employee via email. *Id*. ¶39.

Both Aaron's and its franchisees utilize computer workstations that are maintained by Aaron's. *Id*. ¶41. In order for store employees to access the internet, the workstation's network communications have to pass through a firewall and content filtering system that is also maintained by Aaron's. *Id.*¶42. As part of this system, Aaron's utilizes a "whitelisting" policy, which allows store workstations to access only those internet sites that have been explicitly and intentionally permitted by Aaron's. *Id.* ¶43. According to Dr. Sherr, Aaron's had to affirmatively permit its franchises access to DesignerWare's Web Portal in order for the franchise to activate the PCRA/Detective Mode system. *Id.* ¶45. Once Detective Mode captured information from a customer's computer and forwarded the information to DesignerWare's Server, the DesignerWare Server would forward that information (via email) to Aaron's corporate email server. *Id.* ¶49. Store employees could then access the captured information by accessing the corporate email server using Aaron's intranet. *Id.* Aaron's corporate email server is common to "every single intercept in this system," according to Dr. Sherr. *Id.*

To summarize the foregoing, the various components of Aaron's PCRA/Detective Mode System act in concert to allow (a) a store employee to surreptitiously cause the installation of Detective Mode on a customer's computer, (b) the surreptitious collection of key strokes, screenshots, and (optionally) webcam photos and text-based clip board contents belonging to the computer user and (c) the transfer of the collected information to the store employee's email service using DesignerWare's server as a proxy. *Id*. ¶51. In Dr. Sherr's opinion, these integrated components constitute an "electronic communications interception system." *Id.* Dr. Sherr believes that the PCRA/Detective Mode system's architecture and functionality make it "highly probable" that computer users' electronic communications will be intercepted and transmitted to

store employees. *Id.* ¶52. That is because, when Detective Mode is active, all of the computer user's keypresses are recorded, which will include any and all typed communication. *Id*.

Importantly, Detective Mode does not distinguish between keystrokes that correspond to a communication and those that do not. *Id*. ¶29. However, since Detective Mode intercepts all keystrokes, it captures any keystrokes that belong to any typed communication. *Id.* According to Dr. Sherr, this interception happens as the keystrokes occur. *Id.* That is, the computer user's keystrokes – including (but not limited to) those belonging to email, instant messages, text chat sent during online games, Facebook posts, Twitter "tweets", etc. – are intercepted as they occur and are recorded by the Detective Mode software.[ ] *Id.*

Dr. Sherr's report also addresses the timing of intercepted communications. The PCRA/Detective Mode system captures screenshots of the computer user's internet activity the instant that the screenshot is taken. *Id*. ¶62. Thus, the system will intercept any communications that happen to be on the screen when the screenshot occurs. *Id.* ¶63. This could include screenshots of, e.g., instant messaging, email, online games, and online communications with internet websites. *Id.* ¶62. Because the system also captures keystrokes as they occur, any typed form of communications – such as email, instant messages, and posting to online social network sites – will be intercepted at the time the user inputs the communication. *Id.* ¶64.

Because database entries for a computer only appear in the DesignerWare database if PCRA was running on that computer and was able to contact the DesignerWare database via the internet, Dr. Sherr believes that the DesignerWare database provides a common means of determining which customers connected their computers to the internet, and when they did so. *Id*. ¶65. Dr. Sherr recognizes that "[n]ot all screenshots and keypresses correspond to a communication and it is of course possible for a computer to never be connected to the Internet."

Id. ¶65. However, he also opines that, "[a]s a practical matter, . . . the vast majority of users use the keyboard to communicate on the Internet." *Id.* ¶66. In Dr. Sherr's opinion, even typing a URL into a modern web browser results in a communication of that typed URL to a web server. *Id.* Thus, in Dr. Sherr's view, "[g]iven the popularity of web browsing, email, and instant messaging, it is more probable than not that the overwhelming majority of users who connect to the internet will communicate typed (and therefore intercepted) messages. *Id.*

In conclusion, Dr. Sherr opines that:

> a. Aaron's PCRA/Detective Mode System constitutes an interception system;
>
> b. The intentional whitelisting of DesignerWare's websites facilitated the use of Aaron's PCRA/Detective Mode System;
>
> c. Aaron's PCRA/Detective Mode System captured the electronic communications of the computer users;
>
> d. The intercepted keystrokes were captured as the keys were typed;
>
> e. The captured screenshots depict the contents of a user's screen the instant that the screenshot was taken;
>
> f. The mechanisms used to capture and transmit keystrokes, screenshots, and (optionally) clipboard contents and webcam photos were the same for all users of computers that had an activated Detective Mode from an Aaron's store.

Id. ¶71.

The Defendants filed their respective submissions in opposition to the renewed motion for class certification in November 2016. ECF Nos. 451, 452, 456, 457. The following month, Plaintiffs' filed their materials in reply. ECF No. 463, 465. Thereafter, supplemental filings were accepted by the Court on January 26 and 27, and March 31, 2017. ECF No. 492, 494. 499. Finally, oral argument was held on March 30, 2017. *See* ECF Nos. 498, 501. The relevant issues have now been sufficiently joined and the motion is ripe for adjudication.

B. Federal Rule 23 Standard of Review

The class-action device is an exception to the rule that litigation is usually "'conducted by and on behalf of the individual named parties only.'" *Comcast Corp. v. Behrend*, —— U.S. ——, 133 S. Ct. 1426, 1432 (2013) (quoting *Califano v. Yamasaki*, 442 U.S. 682, 700–01 (1979)). Accordingly, the party proposing class-action certification bears the burden of affirmatively demonstrating by a preponderance of the evidence his compliance with the requirements of Rule 23. *Id*.

To be certified, a class must satisfy the four requirements of Federal Rule of Civil Procedure 23(a): (1) numerosity; (2) commonality; (3) typicality; and (4) adequacy of representation. *See* Fed. R. Civ. P. 23(a); *In re Cmty. Bank of N. Va.*, 418 F.3d 277, 302 (3d Cir. 2005) ("*Community Bank I*"). If the Rule 23(a) requirements are met, the court must then find that the class fits within one of the three categories of class actions set forth in subsection 23(b). *Id.* These include, in relevant part, actions where:

> **(2)** the party opposing the class has acted or refused to act on grounds that apply generally to the class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the class as a whole; or
>
> **(3)** the court finds that the questions of law or fact common to class members predominate over any questions affecting only individual members, and that a class action is superior to other available methods for fairly and efficiently adjudicating the controversy. The matters pertinent to these findings include:
>
> > **(A)** the class members' interests in individually controlling the prosecution or defense of separate actions;
> >
> > **(B)** the extent and nature of any litigation concerning the controversy already begun by or against class members;
> >
> > **(C)** the desirability or undesirability of concentrating the litigation of the claims in the particular forum; and
> >
> > **(D)** the likely difficulties in managing a class action.

Fed. R. Civ. P. 23(b)(2) and (3).

A court evaluating a motion for class certification is obligated to probe behind the pleadings when necessary and conduct a "rigorous analysis" in order to determine whether the Rule 23 certification requirements are satisfied. *In re Hydrogen Peroxide Antitrust Litig*., 552 F.3d 305, 309, 317-18 (3d Cir. 2008), *as amended* (Jan. 16, 2009). In making a class certification ruling, the court has "no license to engage in free-ranging merits inquiries." *Amgen Inc. v. Connecticut Ret. Plans and Trust Funds*, 568 U.S. 455, 466 (2013). Rather, a court can consider merits questions "only to the extent [ ] that they are relevant to determining whether the Rule 23 prerequisites for class certification are satisfied." *Id*. Finally, any factual determinations in support of the court's Rule 23 findings must be made by a preponderance of the evidence. *In re Hydrogen Peroxide*, 552 F.3d at 307.

C. Analysis

As noted, Plaintiffs seek to certify a class defined as:

> All persons who leased and/or purchased one or more computers from Aaron's, Inc. and/or Aspen Way Enterprises, Inc., and their household members, on whose computers Designerware's Detective Mode was installed and activated without such person's consent on or after January 1, 2007.[5]

[5] Plaintiffs posit that the putative class should exclude "the Defendants themselves, any subsidiary of any of the Defendants, any family members of the Defendants who are such customers, all employees and directors of Defendants or any subsidiary, and their legal representatives," as well as "the Court and any members of the Court's staff responsible for the disposition of this action." ECF No. 439 at 1 n.1.

ECF No. 439. They contend that certification is appropriate under either Rule 23(b)(2) or Rule 23(b)(3). We consider each aspect of Rule 23's requirements below.[6]

1. Numerosity

Under Rule 23(a), a threshold requirement for class certification is that the putative class is "so numerous that joinder of all members is impracticable." Fed. R. Civ. P. 23(a)(1). The Third Circuit Court of Appeals has said that, "[n]o minimum number of plaintiffs is required to maintain a suit as a class action, but generally if the named plaintiff demonstrates that the potential number of plaintiffs exceeds 40, the first prong of Rule 23(a) has been met." *Stewart v. Abraham*, 275 F.3d 220, 226–27 (3d Cir. 2001) (citing 5 James Wm. Moore et al., Moore's Federal Practice §23.22[3][a] (Matthew Bender 3d ed.1999)).

Based on an examination of the Detective Mode emails on Aaron's corporate server, Plaintiffs posit that approximately 895 computers had Detective Mode installed and activated on them. Of these, 167 were computers of Aspen Way customers. *See* ECF No. 293-11; *see* also ECF No. 440-9. Plaintiffs assert that this evidence satisfies the numerosity requirement.

Aspen Way contends that Plaintiffs' assertion of numerosity is speculative, however, because Plaintiffs have not established the number of class members who did not consent to the installment of PCRA on their computers. Based on the record as it now stands, this Court finds

[6] Plaintiffs contend that, by virtue of the Third Circuit's prior ruling in this case, it is now the law of this case that their proposed class definition is ascertainable. This Court agrees. In its decision, the Court of Appeals considered a proposed class definition that is, in all material respects, identical to the definition being proposed here. *See Byrd v. Aaron's Inc*., 784 F.3d 154, 160 (3d Cir. 2015). The Third Circuit first concluded that the proposed class definition as not necessarily unascertainable simply because it was under-inclusive. *Id*. at 166-67. It then held that Plaintiff's proposed classes consisting of "owners" and "lessees" are ascertainable. *Id*. at 169. Finally, the Third Circuit held that "household members" of owners or lessees are also ascertainable. *Id*. In view of the Third Circuit's prior ruling, Plaintiffs have satisfied the ascertainability requirement for purposes of certification under Rule 23(b)(3).

no reason to presume that the number of Aspen Way customers who consented to the installation and activation of Detective Mode is so great as to preclude a finding that joinder of all class members will be impracticable. Aspen Way has already admitted in its answer that it did not typically inform its computer lessees about PCRA and its capabilities. ECF No. 354, ¶108. The company made similar admissions in the course of the FTC's investigation. *See* ECF No. 440-8, at ¶¶30-32. Plaintiffs' expert, Dr. Sherr, opines that Detective Mode is designed to be capable of both installing and operating without the user's knowledge. ECF No. 440-2 at 6 n.8. And, while some Aspen Way customers may have consented to the use of Detective Mode in connection with efforts to locate a lost or stolen computer, the available evidence suggests that this was more the exception than the rule.[7] Accordingly, this Court finds that the numerosity requirement is satisfied.

2. Commonality

"A putative class satisfies Rule 23(a)'s commonality requirement if the named plaintiffs share at least one question of fact or law with the grievances of the prospective class." *Rodriguez v. Nat'l City Bank*, 726 F.3d 372, 382 (3d Cir. 2013) (internal quotation marks and

[7] In its supplemental answers to interrogatories, Aspen Way provided a list of approximately eighty-one (81) Aspen Way computers (differentiated by computer identification numbers) on which Detective Mode was activated, along with the reason for the activation. *See* ECF No. 440-9. The information was originally verified by one of Aspen Way's Rule 30(b)(6) representatives, Rohnn Lampi. According to Aspen Way's supplemental answers, some of the Detective Mode activations involved situations where Detective Mode was utilized at the request of the customer after the customer reported the computer stolen or missing. In at least fifty-nine (59) cases, however, the activation was reported to be the result of a customer's apparent payment default rather than reports by the customer of a lost or stolen computer. *See id*. This Court can think of no reason why consent should be presumed in situations where Detective Mode was activated because of a customer's failure to make timely lease payments. In this Court's estimation, a fair and reasonable inference can be drawn that most of the 167 computers on which Detective Mode was activated did not involve activation either at the customer's request or with their consent.

citation omitted). The bar for establishing commonality is "not high." *In re Cmty. Bank of N. Va. Mortgage Lending Practices Litig*. ("*Community Bank III*"), 795 F.3d 380, 397 (3d Cir. July 29, 2015). The relevant inquiry focuses "not on the strength of each class member's claims but instead 'on whether the defendant's conduct was common as to all of the class members.'" *Id*. (quoting *Sullivan v. DB Investments*, 667 F.3d 273, 298 (3d Cir. 2011), and citing other authority). "[A]s long as all putative class members were subjected to the same harmful conduct by the defendant, Rule 23(a) will endure many legal and factual differences among the putative class members." *Community Bank III*, 795 F.3d at 397.

At the same time, however, the claims of each class member must depend upon a "common contention" that is "capable of classwide resolution," meaning that "'determination of its truth or falsity will resolve an issue that is central to the validity of each one of the claims in one stroke.'" *Wal-Mart Stores, Inc. v. Dukes*, 564 U.S. 338, 350 (2011). "What matters to class certification . . . is not the raising of common questions—even in droves—but, rather the capacity of a classwide proceeding to generate common *answers* apt to drive the resolution of the litigation.'" *Id*. (internal quotation marks and citation omitted) (emphasis in the original).

Applying these principles to the facts at issue here, the Court is satisfied that commonality is present. In this case, each of the Defendants engaged in a course of conduct that was generally common to all class members. In addition, the PCRA/Detective Mode system functioned in the same basic manner for all putative class members. In order to present a claim, each class member would have to put on the same general proof as to how information was captured through the Defendants' use of PCRA and Detective Mode, and the respective roles that Aaron's and Aspen Way played in this process. *See In re Nat'l Football League Players' Concussion Injury Litig*., 307 F.R.D. 351, 371 (E.D. Pa. 2015) (commonality factor was present

where defendants engaged in a common course of conduct and "[n]o Class Member could prevail without proving the NFL Parties' misconduct"). One question that may be answered in a common fashion is whether the PCRA/Detective Mode system utilized by Aaron's and Aspen Way constitutes a "device" used for "interception," within the meaning of the ECPA. Resolution of this question will "drive the resolution of the litigation" because liability under the ECPA requires a showing that the Defendants "intercept[ed], endeavor[ed] to intercept[]," or "procure[d] any other person to intercept" electronic communications using a "device." 18 U.S.C. §2511(1)(a). Another common factual question is whether Detective Mode is capable of capturing the computer user's transmission of information in a contemporaneous manner. The answer to this question will drive a resolution of the litigation because the Third Circuit Court of Appeals has held that "an 'intercept' under the ECPA must occur contemporaneously with transmission," *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 113 (3d Cir. 2003) (holding that "a stored e-mail could not be intercepted within the meaning of [the ECPA].").

Aspen Way contends that commonality is lacking "due in part to Plaintiffs' overly broad class definition that sweeps in countless individuals who did not and could not have any electronic communications documented by Detective Mode, not all putative class members are even capable of having suffered the same legal injury." ECF No. 452 at 6. To the extent the class has been defined in an overly broad manner, this particular defect goes to the issue of "predominance," which will be addressed below. *See Byrd*, 784 F.3d at 168 (remarking that the District Court conflated the issue of "ascertainability" with "overbreadth (or predominance), and Article III standing"); *Homes v. Pension Plan of Bethlehem Steel Corp.*, 213 F.3d 124, 137-38 (3d Cir. 2000) (discussing an "overbroad" class as requiring individual determinations that fail to satisfy Rule 23(b)(3)'s predominance requirement). And, to the extent the alleged overbreadth

entails putative members who may not have been injured by the Defendants' alleged wrongdoing – *e.g.*, because they did not use the subject computer or because their "communications" were not contemporaneously intercepted, these discrepancies do not defeat a finding of commonality. Following the Supreme Court's decision in *Dukes*, the Third Circuit Court of Appeals has reiterated that commonality may be present "'even when not all members of the plaintiff class suffered an actual injury, when class members did not have identical claims, and, most dramatically, when some members' claims were arguably not even viable.'" *In re Nat'l Football League Players Concussion Injury Litig*., 821 F.3d 410, 427 (3d Cir.), *as amended* (May 2, 2016), *cert. denied sub nom. Gilchrist v. Nat'l Football League*, --- U.S. ---, 137 S. Ct. 591 (2016), *and cert. denied sub nom. Armstrong v. Nat'l Football League*, --- U.S. ---, 137 S. Ct. 607 (2016) (quoting *Community Bank III*, 795 F.3d at 397). *See also Baby Neal for and by Kanter v. Casey*, 43 F.3d 48, 56 (3d Cir. 1994)("[C]lass members can assert such a single common complaint even if they have not all suffered actual injury; demonstrating that all class members are *subject* to the same harm will suffice.")(emphasis in the original).

Aspen Way next challenges commonality on the ground that the claims of leaseholders will differ from the claims of non-leaseholders. Aspen Way's assumption is that it may be able to show that leaseholders consented to the Defendants' activation of Detective Mode, whereas non-leaseholders could not have consented. Aspen Way also believes that "the analysis of the rationale for activation of Detective Mode would be much different since it was typically the lessee's failure to make required payments that led to the activation of Detective Mode." ECF No. 452 at 7.

The Court is not persuaded that these arguments defeat a finding of commonality. As noted, commonality focuses on whether the defendant's conduct was common as to all class

members, rather than on the relative strength of each class member's claim. *Community Bank III*, 795 F.3d at 397. To the extent individualized distinctions inhere in the class members' claims, the Court addresses them in the context of its predominance and superiority analysis.

3. Typicality

The third threshold requirement under Rule 23(a) is that the plaintiffs' claims must be typical of those of other class members. "The concepts of typicality and commonality are closely related and often tend to merge." *In Marcus v. MVW of N. Am., LLC*, 687 F.3d 583, 597 (3d Cir. 2012)(citing *Baby Neal v. Casey*, 43 F.3d at 56). "Typicality, however, derives its independent legal significance from its ability to 'screen out class actions in which the legal or factual position of the representatives is markedly different from that of other members of the class even though common issues of law or fact are present.'" *Id.* at 598 (quoting 7A Charles Alan Wright et al., Federal Practice and Procedure § 1764 (3d ed. 2005)).

In assessing whether the representative plaintiff is "markedly different" from the class as a whole, courts examine the attributes of the plaintiff, the proposed class, and the similarity between the two. *Id*. (citation omitted). Specifically, courts consider three "distinct," but "related" concerns:

> (1) the claims of the class representative must be generally the same as those of the class in terms of both (a) the legal theory advanced and (b) the factual circumstances underlying that theory; (2) the class representative must not be subject to a defense that is both inapplicable to many members of the class and likely to become a major focus of the litigation; and (3) the interests and incentives of the representative must be sufficiently aligned with those of the class.

Id. (quoting *In re Schering Plough Corp. ERISA Litig.*, 589 F.3d 585, 599 (3d Cir. 2009)). "If a plaintiff's claim arises from the same event, practice or course of conduct that gives rise to the claims of the class members, factual differences will not render that claim atypical if it is based

on the same legal theory as the claims of the class." *Id.* (citation omitted). The threshold for establishing "typicality" is therefore "low." *Nat'l Football League Players Concussion Injury Litig.*, 821 F.3d at 428.

In this case, the requirements of typicality are met. First, the claims of the class representatives are generally the same as those of the class as a whole, both in terms of the legal theory being advanced and the factual circumstances underlying the theory. Plaintiffs, like the absent class members, are asserting alleged violations of the ECPA. Moreover, the Plaintiffs' ECPA claims and the ECPA claims of putative class members arise from the same event – namely, the activation of Detective Mode on the subject computers leased or purchased from Aspen Way. Second, there are no particular defenses to which the named Plaintiffs are uniquely subject. Third, the interests and incentives of the Plaintiffs are sufficiently aligned with those of other putative class members.

In challenging the "typicality" prong of certification, Aspen Way points out that "Crystal Byrd, having paid off her computer in full, was the rightful owner of her computer at the time of the alleged Detective Mode activation, which was requested [by Aspen Way] on the mistaken belief that she had defaulted on her lease agreement." ECF No. 452 at 10. "Because she owned the computer at the time of the Detective Mode activation," *id.*, Aspen Way insists that "the Byrd's' [sic] claims will be remarkably atypical of the legal claims of the class as a whole." *Id.* This appears to be a distinction without any legal relevance, as Aspen Way cites no authority for the proposition that the delinquency of a leaseholder's account provides a defense from liability under the ECPA. Nor does Aspen Way point to any provision in its lease agreements that would provide grounds to conclude that delinquent customers of Aspen Way expressly consented to the installation and activation of Detective Mode on their computers.

Aspen Way also asserts that certain of its customers requested activation of Detective Mode in order to obtain help locating lost or stolen computers. Although (as discussed below) this contingency presents concerns as to predominance, it does not necessarily defeat a finding of typicality. To the extent it can be established that a particular leaseholder or computer owner requested activation of Detective Mode, that individual would, by definition, be excluded from the class. Typicality among the remaining class members would be preserved, however.

Aspen Way next argues that the class, as defined, is overbroad and may include individuals who did not use the computers in question, as well as individuals whose intercepted content was significantly different from the content that was captured from the Byrds' computer. As discussed, however, the alleged overbreadth of the class is a consideration more relevant to the "predominance" inquiry. And, to the extent that captured content may have varied among class members, these variations are not significant enough to defeat typicality where the underlying course of conduct on the part of the Defendants and the underlying legal theories are the same for both the named representative and the absent class members. *Nat'l Football League Players Concussion Injury Litig*., 821 F.3d at 428 ("Even relatively pronounced factual differences will generally not preclude a finding of typicality where there is a strong similarity of legal theories or where the claim arises from the same practice or course of conduct.")(internal quotation marks and citation omitted).

At bottom, the typicality requirement "ensures the interests of the class and the class representatives are aligned so that the latter will work to benefit the entire class through the pursuit of their own goals." *Id*. at 427-28 (internal quotation marks and citation omitted). Based on the record at hand, this Court finds that Plaintiffs' interests and those of the class are

sufficiently aligned such that the Plaintiffs, in prosecuting their own claims, will work to benefit the class as a whole.

4. Adequacy of Representation

Rule 23(a)'s fourth threshold requirement is that the representative plaintiffs must "fairly and adequately protect the interests of the class." Fed. R. Civ. P. 23(a)(4). The adequacy requirement concerns both "the experience and performance of class counsel" and "the interests and incentives of the representative plaintiffs." *Dewey v. Volkswagen Aktiengesellschaft*, 681 F.3d 170, 181 (3d Cir. 2012) (citing *Community Bank I*, 418 F.3d at 303). "'The principal purpose of the adequacy requirement is to determine whether the named plaintiffs have the ability and the incentive to vigorously represent the claims of the class.'" *Community Bank III*, 795 F.3d at 393 (quoting *In re Cmty. Bank of N. Va. ("Community Bank II")*, 622 F.3d 275, 291 (3d Cir. 2010)). "'[T]he linchpin of the adequacy requirement is the alignment of interests and incentives between the representative plaintiffs and the rest of the class.'" *Id*. (quoting *Dewey*, 681 F.3d at 183).

In this case, the Byrds' interests and incentives to prosecute their case are adequately aligned with the interests and incentives of absent class members, such that the requirements of Rule 23(a)(4) are satisfied. As Plaintiffs observe, they and the absent class members have a common interest in proving that the ECPA was violated. Plaintiffs have demonstrated their commitment to the class objectives by agreeing to prosecute their claims in this forum, by traveling here to attend the Court's May 24, 2011 preliminary injunction hearing, and by submitting to depositions in connection with the litigation. Nothing in the record suggests to this Court that Plaintiffs' interests in the litigation will be antagonistic to the interests of other class members.

Nevertheless, Aspen Way challenges the Byrds' adequacy as class representatives based, once again, on the fact that Crystal Byrd owned her computer outright at the time that Detective Ware was installed and activated on it. According to Aspen Way, Crystal Byrd's ownership of the computer renders moot any consent she gave at the time she signed her lease, and frees her of the "struggle to overcome Aspen Way's superior contractual right to possession and control of the computer upon default or delinquency by the lessee . . . ." ECF No. 452 at 12. In sum, Aspen Way reasons that the Byrds have not suffered the same injury as putative class members, and their interests fail to align with the interests of the class because they have "no stake in evidence that is critical to the establishment of the claims of other putative class members . . . ." *Id.*

This argument is unpersuasive. First, to the extent that Plaintiffs' ECPA claims are arguably stronger than the claims of other putative class members, this consideration seemingly weighs in favor of – not against -- a finding of Plaintiffs' adequacy. Second, by virtue of the manner in which the putative class has been defined, each and every member will necessarily be asserting that he/she did not consent to the installation or activation of Detective Mode on the computer at issue. This fact places the Byrds in alignment with absent class members. There is no reason to presume (as Aspen Way suggests) that Plaintiffs "have no stake" in contesting class members' consent on a class-wide basis. *See* ECF No. 452 at 12. Third, the legal relevance of Crystal Byrd's ownership interest in her computer vis-a-vis other class members who may have been leaseholders, or even delinquent leaseholders, is dubious for the reasons discussed. Nowhere in its brief has Aspen Way provided any legal authority to support its implicit assumption that it will be absolved of any liability under the ECPA if the particular computer at issue was in the custody of a delinquent lessee. For all of these reasons, the fact that Crystal

Byrd owned her computer at the time of the allegedly unlawful interceptions does not make her (or her husband) an inadequate class representative.

Aaron's does not contest the adequacy of Plaintiffs as class representatives, but it does contest the adequacy of class counsel. Aaron's objection in this regard stems from the involvement of Plaintiffs' counsel in filing other lawsuits against the Defendants in other jurisdictions based on the same underlying facts.

In this regard, the undersigned notes that the Plaintiffs in this case are represented by no less than a dozen different attorneys hailing from numerous different law firms. One of Plaintiffs' attorneys, Andrea S. Hirsch, Esq., is involved in two separate lawsuits in Georgia state court, *Price v. Aaron's Inc. and NW Freedom Corp., d/b/a Aaron's Sales and Leasing, see* ECF No. 451-8, and *Sneed v. SEI/Aaron's, Inc., d/b/a/ Aaron's Sales and Leasing*, *see* ECF No. 451-14. Ms. Hirsch and three other of Plaintiffs' attorneys – Edward C. Konieczney, Esq., Frederick S. Longer, Esq., and Maury A. Herman, Esq. – are involved in *Peterson v. Aaron's, Inc. and Aspen Way Enterprises, Inc.*, the putative class action filed in the U.S. District Court for the Northern District of Georgia. *See* ECF No. 451-13. Another member of the Plaintiffs' legal team, John H. Robinson, Esq., also represents individual plaintiffs in three separate lawsuits filed in Wyoming state court: *Kinion v. Aspen Way Enterprises, Inc.*, ECF No. 451-5; *Howard v. Aspen Way Enterprises, Inc.*, ECF No. 451-6; and *Winn v. Aspen Way Enterprises, Inc.*, ECF No. 451-7. None of these other lawsuits involves claims asserted under the ECPA.

"Like a lawyer in any litigation, a class action attorney may not simultaneously represent two clients if those clients' interests are directly adverse or if there is significant risk that the dual representation will materially limit the lawyer's representation of one client." W. Rubenstein, NEWBERG ON CLASS ACTIONS § 3:75 (5th ed. 2015). However, "only client conflicts that are

material and presently manifest—rather than merely trivial, speculative, or contingent on the occurrence of a future event—will affect the adequacy of class counsel." *Id.* As a general rule,

> class counsel may represent multiple sets of litigants—whether in the same action or in a related proceeding—so long as the litigants' interests are not inherently opposed.[ ] Indeed, courts have recognized that concurrent representation may enable counsel to leverage a better settlement for both sets of plaintiffs due to a defendant's desire to obtain a global resolution.[ ] Representing multiple clients in parallel proceedings will also benefit the class to the extent that class counsel gain useful legal and factual knowledge in pursuing the concurrent action.[ ]

Id. (internal footnotes omitted). Problems can arise where, for example, class counsel represents two sets of claimants, both of whom have an interest in recovery from a limited fund. *See, e.g., In re Cardinal Health, Inc. ERISA Litigation,* 225 F.R.D. 552, 557 (S.D. Ohio 2005) (stating that "[c]ounsel cannot represent different classes of plaintiffs with conflicting claims who are seeking recovery from a common pool of assets"); *LeBeau v. U.S.*, 222 F.R.D. 613, 618 (D.S.D. 2004) (attorney could not adequately represent putative class where he previously represented a group of litigants who were eligible to draw from the same judgment fund). "Where multiple, separate counsel jointly represent the class, . . . absent an actual conflict[,] the simultaneous representation of individuals or another class by a member of the counsel group against the same defendants is not disqualifying.[ ]" 1 Joseph M. McLaughlin, MCLAUGHLIN ON CLASS ACTIONS §4:39 (9th ed. 2012).

Based on the record at hand, this Court finds no obvious or inherent conflict of interest in the instant case that would preclude Plaintiffs' attorneys from adequately representing absent class members. Aaron's argues that putative class counsel "suffer from insurmountable conflicts of interest" as the result of having filed the putative class action in *Peterson*, ECF No. 451 at 31, but class certification in that case has already been denied and it does not appear that Plaintiffs' lawyers are appealing that ruling. At this juncture, this Court is not faced with litigants

competing for recovery from a limited fund. Plaintiffs in this putative class action are only seeking recovery under the ECPA – a legal theory which is not being pursued in the other pending case, and only for alleged violations stemming from the activation of Detective Mode on Aspen Way computers. Nor are any other patent and material conflicts present. Accordingly, this Court is satisfied that the requirements of Rule 23(a)(4) have been met.

5. Predominance of Common Issues

Having determined that the preliminary criteria for certification under Rule 23(a) have been satisfied in this case, the Court will next consider whether certification is appropriate under Rule 23(b). As noted, Plaintiffs seek certification under Rule 23(b)(3), pursuant to which issues that are common to the class must predominate over individual issues. *Community Bank III*, 795 F.3d 380, 399.[8] This requirement imposes a "far more demanding" standard than the commonality requirement of Rule 23(a). *Id*. (quoting *Amchem Prod., Inc. v. Windsor*, 521 U.S. 591, 623–24 (1997)).

At bottom, the predominance criterion "'tests whether proposed classes are sufficiently cohesive to warrant adjudication by representation.'" *Community Bank III*, 795 F.3d at 399 (quoting *Amchem*, 521 U.S. at 623). "To determine this level of cohesion, 'the predominance requirement focuses on whether essential elements of the class's claims can be proven at trial with common, as opposed to individualized, evidence.'" *Taha v. Cty. of Bucks*, 2017 WL 2871757, at *12 (3d Cir. July 6, 2017) (quoting *Hayes v. Wal-Mart Stores, Inc*., 725 F.3d 349,

[8] The Supreme Court has explained that:

> An individual question is one where members of a proposed class will need to present evidence that varies from member to member, while a common question is one where the same evidence will suffice for each member to make a prima facie showing [or] the issue is susceptible to generalized, class-wide proof.

Tyson Foods, Inc. v. Bouaphakeo, ––– U.S. –––, 136 S. Ct. 1036, 1045 (2016) (internal quotation marks omitted).

359 (3d Cir. 2013)); *see also Neale v. Volvo Cars of N. Am., LLC*, 794 F.3d 353, 370 (3d Cir. 2015) ("Predominance 'begins, of course, with the elements of the underlying cause of action.'") (quoting *Erica P. John Fund, Inc. v. Halliburton Co*., 563 U.S. 804, 809 (2011)). "'Because the nature of the evidence that will suffice to resolve a question determines whether the question is common or individual, a district court must formulate some prediction as to how specific issues will play out in order to determine whether common or individual issues predominate in a given case.'" *Marcus*, 687 F.3d at 600 (quoting *In re Hydrogen Peroxide Antitrust Litig*., 552 F.3d at 311).

In this case, Plaintiffs' only claim asserts direct violations of the ECPA. "A plaintiff pleads a prima facie case under the [ECPA, 18 U.S.C. §2511(1)(a)] by showing that the defendant '(1) intentionally (2) intercepted, endeavored to intercept or procured another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication, (5) using a device.'" *In re Nickelodeon Consumer Privacy Litig*., 827 F.3d 262, 274 (3d Cir. 2016) (quoting *In re Google Inc. Cookie Placement Consumer Privacy Litig*., 806 F.3d 125, 135 (3d Cir. 2015)), *cert. denied sub nom. C. A. F. v. Viacom Inc*., --- U.S. ---, 137 S. Ct. 624 (2017). For purposes of the ECPA, the "intercept" must occur contemporaneously with the transmission of the electric communication. *Fraser*, 352 F.3d at 113.

Central to the claims of every class member is the question whether the Defendants intercepted (or endeavored or procured another to intercept) the "contents" of the class member's "electronic communication." Because this central liability question requires individualized proof, and because it predominates over other issues common to the putative class, certification under Rule 23(b)(3) is inappropriate.

In part, the need for individualized inquiries stems from the overly broad manner in which the class has been defined, *to wit*: "All persons who leased and/or purchased one or more computers from Aaron's, Inc. and/or Aspen Way Enterprises, Inc., and their household members, on whose computers Designerware's Detective Mode was installed and activated without such person's consent on or after January 1, 2007." ECF No. 439. The definition is not tied to computer users *per se*, but rather to lessors and purchasers of the subject computers and their household members. As the district court observed in *Peterson v. Aaron's, Inc.,* 2017 WL 364094, at *3 (N.D. Ga. Jan. 24, 2017), "[t]he proposed class includes numerous household members . . . who have not been injured and thus have no cause of action." *See* ECF No. 492-1 at p. 9.[9] For example, the class encompasses household members who may have never used the computers, or those who may have used them, but not at a time when Detective Mode was activated. The class also includes individuals who leased or purchased one of the subject computers for the benefit of another person not living within the household, such as a parent who may have acquired the computer for the benefit of an independent child. "Exacerbating this problem," as the *Peterson* court observed, "is the fact that the [class] definition provides no end date." *Peterson,* 2017 WL 364094, at *3. Instead, Plaintiffs simply state that the class extends from any point on or after January 1, 2007. "As a result, the class includes all household members . . . of a computer lessee or purchaser since [January 1, 2007], even though some household members . . . may not overlap with the period of time the computer was used . . . ." *Id.* In any of these situations, the putative class members would not have been injured by the

[9] The *Peterson* court addressed the overbreadth problem in the context of addressing ascertainability. Pursuant to the Third Circuit's directive in *Byrd,* 784 F.3d at 168-69, we address the problem in the context of "predominance."

Defendants' conduct, and therefore could not possibly state a claim; however, culling these individuals from the pool of plausible claimants will require particularized inquiry.

Apart from determining *whose* information was captured (in order to identify the relevant computer users), the parties will have to examine *what* information Detective Mode captured in order to determine, in any given case, whether the information at issue constitutes an electronic "communication" within the meaning of the ECPA. Under the Act, an "electronic communication" is generally defined to mean "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce . . . ." *See* 18 U.S.C. §2510(12). While the transmission of a Facebook post or an email message over the internet likely meets this definition, other computer-related activities – such as making entries to a computerized calendar or utilizing a word processing application – presumably do not. An examination of the specific content and character of any given screen shot or keystroke is therefore critical to a determination of liability.

Plaintiffs also must establish that the intercept of the electronic communication occurred contemporaneously with its transmission. *See Fraser*, 352 F.3d at 113 (holding that employer's actions in surreptitiously accessing its employee's email from its central file server did not constitute a violation of ECPA because the intercept did not occur at the initial time of the email's transmission). Thus, a screenshot of an email that is being constructed for intended transmission over the internet does not constitute an unlawful interception if the screenshot does not occur contemporaneously with the email's transmission. Similarly, a keystroke log that contemporaneously documents the user's construction of an email does not give rise to liability under the ECPA if the email is ultimately discarded instead of being sent, or is merely saved on

the computer's hard drive in draft form, or is sent at a later time when Detective Mode is not activated.[10] *See, e.g., United States v. Ropp*, 347 F. Supp. 2d 831 (C.D. Cal. 2004) (defendant's interception of keystrokes from the user's keyboard to the computer's processing unit did not constitute unlawful interception of an electronic communication, where interception occurred prior to the communication being transmitted to outside parties by a system affecting interstate or foreign commerce).

Plaintiffs insist that information taken from DesignerWare's database provides a common means of determining which customers connected their computers to the internet and when they did so. Despite having the burden of proving that common issues predominate in this case, Plaintiffs do not specify exactly how this reservoir of information will allow them to prove actual interceptions of various class members' communications on a common, classwide basis. It is presumably Plaintiffs' intention to cull the DesignerWare database for actionable interceptions of electronic communications, then cross-reference that information against Aspen Way's database of consumer information in order to identify the relevant owner or leaseholder of the computer in question. From there, Plaintiffs will presumably attempt to pinpoint the individuals who were

[10] The inquiry is further complicated by the fact that Detective Mode could be utilized in different ways depending on the features that were activated for a particular computer. According to Aspen Way's "Response to Civil Investigative Demand," Detective Mode offered four options: Option One transmitted 30 screen shots, with each one taken at one-second intervals starting at the time of log-in. ECF No. 440-8 at ¶13. Option Two transmitted continuous screen shots of the user's activities. *Id*. Option Three prompted the user to type identifying information into a license form and then transmitted the user's keystrokes to the Designerware Server. *Id*. Option Four shut down the computer and provided a separate option to transmit a web-cam photo. *Id*. Dr. Sherr describes the program slightly differently. Quoting DesignerWare's manual, Dr. Sherr states that Detective Mode would "record all the keys typed and take[ ] a screen shot every two (2) minutes" for a period of up to one hour. ECF No. 442, ¶27. Dr. Sherr also notes, however, that another document entitled "The Detective Program" describes operating modes that continually monitor the computer user's activity without conforming to the one-hour time window. *Id*. ¶28. In sum, the record suggests that Aspen Way's selection of particular Detective Mode features varied from computer to computer depending on the circumstances of each customer's situation.

actually involved in the underlying communications. But even if Plaintiffs are able to sift through the database of interceptions and winnow out those that they believe were contemporaneously intercepted electronic communications, it will still be necessary for the parties to engage in numerous individualized inquiries along the way in order to test Plaintiffs' proof. Ultimately, a violation of 18 U.S.C. §2511(1)(a) cannot be proven without reference to the specific content of each intercepted "communication." Individualized inquiries will be necessary in order to establish: (i) whether any given piece of captured information represents an "electronic communication," (ii) which putative class member is associated with the alleged communication, and (iii) whether the interception occurred "contemporaneously" with transmission. Consequently, this Court is not persuaded that Plaintiffs have demonstrated an ability to establish the predominant issues in their case through common proof.

To the extent that consent is a relevant defense in this case, it too involves fact-specific inquiries that defy common proof. *See* 18 U.S.C. §2511(d) (establishing consent as an affirmative defense). Plaintiffs deny that consent is a legally relevant or factually supportable issue in this case. From a factual standpoint, they contend that an *absence* of consent should be inferred on a classwide basis because the Defendants secretly installed PCRA and Detective Mode on the subject computers. From a legal standpoint, Plaintiffs contend that class certification is appropriate even if Defendants can point to a few customers who consented to the use of Detective Mode. They cite to the Supreme Court's ruling in *Halliburton v. Erica P. John Fund,* 134 S. Ct. 2398 (2014), wherein the Court noted that "pick[ing] off the occasional class member here or there through individualized rebuttal does not cause individual questions to predominate." *Id.* at 2412.

Based on the record at hand -- especially Aspen Way's answer to the Corrected Third Amended Complaint, it is fair to assume that Aspen Way "did not typically inform its computer lessees about PC Rental Agent® and its capabilities." ECF No. 354, ¶108. Nevertheless, the Court is not persuaded that the issue of consent is factually and legally irrelevant to the predominance analysis. Here, there is evidence to suggest that at least some of Aspen Way's customers may have been informed about Detective Mode's capabilities (particularly the program's ability to assist in locating lost or stolen computers) at the time they leased their computers. *See* ECF No. 442-3, Pollock Dep. at 81:24-90:22; *see also* ECF No. 440-9 at 10-12. In fact, the record suggests that Detective Mode was employed most commonly to aid with collection or repossession efforts in the case of delinquent accounts and to assist in the recovery of lost or stolen computers. *See* ECF No. 440-9. In the latter situation, where Detective Mode was activated after customers had reported lost or stolen computers, it appears the activation was sometimes done at the customer's request. *Id.* at 10-12. If Detective Mode was installed on a lost or stolen computer after Aspen Way received the consent of the customer, then no recovery will be possible because Aspen Way will have a valid defense and, in any case, the customer would fall outside the class as it is presently defined. And, even if the customer's consent was *not* obtained but Detective Mode was nevertheless installed in an effort to retrieve a lost or stolen computer, it is likely that any electronic communications that were intercepted thereafter would be those of unauthorized third parties, rather than of class members. In any case, determinations of this kind will require particularized investigations that are not amenable to classwide resolution.

Plaintiffs' other legal theories under the ECPA will require similar individualized proof. In addition to asserting an unlawful interception claim under 18 U.S.C. §2511(1)(a), Plaintiffs

have asserted violations of §2511(1)(c) and §2511(1)(d). ECF No. 296 at ¶¶159-160. Subsection (1)(c) makes it unlawful for a person to "intentionally disclose[ ], or endeavor[ ] to disclose, to any other person the contents of any . . . electronic communication, knowing or having reason to know that the information was obtained through the interception of a[n] . . . electronic communication in violation of this subsection . . . ." 18 U.S.C. §2511(1)(c). Subsection (1)(d) makes it unlawful to "intentionally use[ ], or endeavor[ ] to use, the contents of any . . . electronic communication, knowing or having reason to know that the information was obtained through the interception of a[n] . . . electronic communication in violation of this subsection . . . ." 18 U.S.C. §2511(1)(d). To establish violations of these provisions, Plaintiffs will have to show -- with respect to each class member -- that the Defendants used or disclosed (or endeavored to use or disclose) the class member's unlawfully intercepted communications. Plaintiffs have made no showing in their proposed trial plan as to how they intend to collectively prove these claims.

The parties in this case dispute whether damages could feasibly be addressed on a classwide basis. Plaintiffs contend that the availability of statutory damages makes any individualized monetary calculation unnecessary. Defendants insist that Plaintiffs' trial plan for the damages phase ignores individualized issues and violates the Rules Enabling Act. In this Court's estimation, it is unnecessary to resolve the parties' dispute because, even if damages can be established on a classwide statutory basis, other individualized issues pertaining to liability, as set forth above, predominate in this case, making certification under Rule 23(b)(3) inappropriate.

6. Superiority of Class Action

In order to certify a class under Rule 23(b)(3), the Court must first find that "a class action is superior to other available methods for fairly and efficiently adjudicating the

controversy." Fed. R. Civ. P. 23(b)(3). Pertinent considerations include: "(A) the class members' interests in individually controlling the prosecution or defense of separate actions; (B) the extent and nature of any litigation concerning the controversy already begun by or against class members; (C) the desirability or undesirability of concentrating the litigation of the claims in the particular forum; and (D) the likely difficulties in managing a class action." *Id*. "'The superiority requirement asks a district court to balance, in terms of fairness and efficiency, the merits of a class action against those of alternative available methods of adjudication.'" *Community Bank III*, 795 F.3d at 409 (quoting *Community Bank I*, 418 F.3d at 309).

In this case, consideration of the relevant factors counsel against class certification. As the court in *Peterson* recognized, "several putative class members have filed their own individual lawsuits, which demonstrates the putative class members may have a strong interest in controlling their own litigation." *Peterson*, 2017 WL 364094, at *10. At this point, it appears that at least six separate lawsuits are pending against Aaron's and/or Aspen Way. *See* ECF Nos. 451-5 through 451-8, 451-13, and 451-14. Plaintiffs point out that none of the other pending lawsuits involve claims under the ECPA, but that does not necessarily support the case for certifying a class. The fact that individual plaintiffs have chosen to pursue state theories rather than a federal ECPA claim may simply suggest that they do not feel strongly invested in the federal cause of action. This conclusion is buttressed by the fact that at least one individual plaintiff, Lomi Price, has filed state claims in Georgia and intends to opt out of this litigation if it is certified. *See* ECF No. 451-16.

It is also noteworthy that, of the lawsuits that have been filed to date, this case is the only one filed in Pennsylvania, which suggests that it may not be desirable to concentrate the litigation in this forum. In fact, the undesirability of this forum is one of the factors Lomi Price

cites as a reason for opting out of this case, should it be certified as a class action. *See* ECF No. 451-16 at ¶7. This litigation was originally commenced in the Western District of Pennsylvania only because DesignerWare was located here. Although originally named as a Defendant in this litigation, DesignerWare has since filed for bankruptcy protection and is no longer a party to this case. Most of the lawsuits involving these Defendants have been filed either in Georgia, where Aaron's is headquartered, or in Wyoming, where Aspen Way does business. *See* ECF Nos. 451-5, 451-6, 451-7, 451-8, 451-13, 451-14.

Finally, the predominant individualized issues in the case are likely to present difficulties in managing a class action. In light of these circumstances, this Court cannot say that class action litigation is a superior means of fairly and efficiently adjudicating the parties' controversy.

7. Appropriateness of Certification under Rule 23(b)(2)

Plaintiffs also seek certification of the class for purposes of obtaining injunctive relief under Rule 23(b)(2). This subsection applies where "the party opposing the class has acted or refused to act on grounds that apply generally to the class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the class as a whole . . . ." Fed. R. Civ. P. 23(b)(2).

"Subsection (b)(2) class actions are 'limited to those class actions seeking primarily injunctive or corresponding declaratory relief.'" *Barnes v. Am. Tobacco Co.*, 161 F.3d 127, 142 (3d Cir. 1998) (quoting 1 Newberg on Class Actions § 4.11, at 4–39). Here, Defendants contend, and this Court agrees, that certification under subsection (b)(2) is inappropriate because monetary relief is the focus of Plaintiff's operative pleading. This fact alone counsels against Rule 23(b)(2) certification. *See In re Processed Egg Prod. Antitrust Litig.*, 2017 WL 2791526, at *3 (E.D. Pa. June 27, 2017) (observing that "several courts have denied class certification of

similar proposed 23(b)(2) classes on this financial goal finding alone," and citing authority). *See also Dukes*, 564 U.S. at 363 ("In the context of a class action predominantly for money damages we have held that absence of notice and opt-out violates due process.").

In addition, as Defendants point out, there is no serious risk of irreparable future harm to class members because Defendants have entered into consent decrees that prohibit them from engaging in the very conduct Plaintiff seeks to prosecute in this litigation. *See In re Processed Egg Prod. Antitrust Litig.*, 2017 WL 2791526, at *4 ("To demonstrate cohesiveness [for purposes of Rule 23(b)(2) certification], Plaintiffs must show that the following elements are susceptible of common proof: (1) actual or threatened injury from an impending violation of the antitrust laws or from a contemporary violation likely to continue or recur; (2) causation; and (3) likelihood that the equitable relief will redress the injury.") (internal quotation marks and citation omitted). *See also Peterson,* 2017 WL 364094, at *11 (declining to certify plaintiffs' case under Rule 23(b)(2) for purposes of issuing "a Court-approved notice to the class that their computers are laden with spyware" where there was "little to no risk of continuing injury" to class members because Aaron's had entered into consent decrees with the Federal Trade Commission agreeing to cease any use of the monitoring software at issue).

Plaintiffs contend that injunctive relief is warranted because class members have the right to express notice that their rights under the ECPA were violated. This argument is unpersuasive. As Defendants correctly point out, Aaron's settlement with the Federal Trade Commission was a matter of public record and received considerable national publicity. In the absence of more compelling circumstances, certification under Rule 23(b)(2) is not warranted.

III. CONCLUSION

For the foregoing reasons, it is respectfully recommended that Plaintiffs' renewed motion to certify the class [ECF No. 439] be DENIED.

In accordance with 28 U.S.C. §636(b)(1) and Fed. R. Civ. P. 72, the parties must seek review by the district court by filing Objections to the Report and Recommendation within fourteen (14) days of the filing of this Report and Recommendation, or by **August 18, 2017.** Any party opposing the Objections shall have fourteen (14) days from the date of service of the Objections to respond thereto, or by **September 1, 2017.** *See* Fed. R. Civ. P. 72(b)(2). **Extensions of time will not be granted in either regard.** Failure to file timely objections may constitute a waiver of appellate rights. *See Brightwell v. Lehman,* 637 F.3d 187, 193 n.7 (3d Cir. 2011); *Nara v. Frank,* 488 F.3d 187 (3d Cir. 2007).

/s/ Susan Paradise Baxter
SUSAN PARADISE BAXTER
United States Magistrate Judge

Dated: August 4, 2017